UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/821,435	04/09/2004	Prasanna J. Satarasinghe	31426.51	1235

75172 7590 10/17/2008

Client 21058
c/o DARBY & DARBY P.C.
P.O. BOX 770
CHURCH STREET STATION
NEW YORK, NY 10008-0770

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
10/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/821,435	SATARASINGHE ET AL.	
	Examiner	Art Unit	
	BENJAMIN E. LANIER	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 August 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 15 August 2008 has been entered.

Response to Amendment

2. Applicant's amendment filed 15 July 2008 amends claims 1, 10-11, 14, 19-20. Applicant's amendment has been fully considered and entered.

Response to Arguments

3. Applicant argues, "Combining Lupper with Chang does not provide a one-time use session password." This argument is not persuasive because the password is essentially only a one-time password (see explanation below), which is clearly disclosed by the proposed combination of Lupper in view of Chang.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 1-20 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant

art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The specification does not disclose one-time entropy generated session passwords. Applicant contents that "The present application discloses 'unique session keys' (Abstract), which are used to derive passwords, therefore passwords are unique to sessions." The specification does not disclose generating the passwords utilizing session keys.

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 1-20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

8. The claims require "one-time entropy generated session password", which renders the claims indefinite because it is unclear how the password could be both a one-time password and a session password. In addition, the password is used solely for the purposes of authenticating the client. Therefore, the password would only be used once for a given session to begin with. At the point the user would need to re-authenticate, a new session would have begun. For the purposes of examination, the password will be treated as a one-time password.

9. Claim 20 requires derivation of the following, "password = F(generating a hash value(Username | n*Value | "sim direct"))," which renders the claims indefinite because the value "n" and "sim direct" are undefined by the claims. Therefore, no claim scope can be obtained.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

12. Claims 1-6, 14, 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lupper, U.S. Publication No. 2003/0171112, in view of Chang, U.S. Patent No. 6,715,082. Referring to claim 1, Lupper discloses a generic WLAN architecture wherein a subscriber name and password are obtained from the subscriber and compared to locally available subscriber data records ([0078]), which meets the limitation of creating a password for a client, storing the password and identification information of the client on a public wireless local area network. The subscriber name and password are compared with the data records to determine whether the subscriber can use services in the local area network ([0080]), which meets the limitation of utilizing the password and the client identity information to authenticate the client in the public wireless local area network. Lupper does not disclose that the passwords are one-time entropy passwords. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use one-time entropy passwords in the WLAN of Lupper in order to

reduce the security risks that are introduced from using fixed user information by using single use passwords that cannot be reused by an intruder as taught by Chang (Col. 2, lines 12-24).

Referring to claim 2, Lupper discloses utilizing the RADIUS protocol ([0083]), which meets the limitation of the authentication is provide by a Remote Authentication Dial-In User Server (RADIUS) server.

Referring to claims 3-5, Lupper discloses that authentication includes utilizing a SIM card in communications with a server ([0092]), which meets the limitation of authenticating the client by a server associated with said WPAN based on a smart card/universal subscriber identity module card/subscriber identity module card.

Referring to claim 6, Lupper discloses that a database exists for billing purposes with respect to the services ([0080]), which meets the limitation of modifying accounting data from the public wireless local area network to include charging data record fields for the client.

Referring to claim 14, Lupper discloses a generic WLAN architecture wherein a subscriber name and password are obtained from the subscriber and compared to locally available subscriber data records ([0078]), which meets the limitation of a first adapter for generating a password for the client. The subscriber name and password are compared with the data records to determine whether the subscriber can use services in the local area network ([0080]). Authentication is performed by a RADIUS server ([0051]), which meets the limitation of wherein the password is used for authenticating the client by a Remote Authentication Dial-In User Service (RADIUS) server. Lupper discloses that authentication includes utilizing a SIM card in communications with a server ([0092]), which meets the limitation of a smart card for a client. Lupper does not disclose that the passwords are one-time passwords. However, it would

have been obvious to one of ordinary skill in the art at the time the invention was made to use one-time entropy passwords in the WLAN of Lupper in order to reduce the security risks that are introduced from using fixed user information by using single use passwords that cannot be reused by an intruder as taught by Chang (Col. 2, lines 12-24).

Referring to claim 15, Lupper discloses that authentication includes utilizing a SIM card in communications with a server ([0092]), which meets the limitation of a second adapter for authenticating the client by a second server based on the smart card.

13. Claims 7-11, 16, 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lupper, U.S. Publication No. 2003/0171112, in view of Chang, U.S. Patent No. 6,715,082, and in further view of Lupien, U.S. Patent No. 6,463,055. Referring to claims 7-9, 16, Lupper does not disclose where or how the passwords are generated. Lupien discloses a wireless network authentication system wherein a password is generated at a first station and compared with a password generated by a mobile terminal using the IMSI of the mobile terminal to authenticate the mobile terminal to access the network (Col. 10, line 56 – Col. 11, line 10), which meets the limitation of creating is independently performed by each of two entities, creating comprises utilizing international mobile subscriber identity (IMSI) of the client, creating comprises utilizing a pseudonym of the client, the first and second adapters reside on separate devices, a fourth adapter for generating the password for the client. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute the password of Lupper with the password of Lupien because such a modification would have yielded the predictable result of mobile terminal authentication.

Referring to claims 10-11, Lupper does not disclose where or how the passwords are generated. Lupien discloses a wireless network authentication system wherein a password is generated utilizing cipher keys (Col. 10, lines 58-61), which meets the limitation of creating comprises utilizing Point-to-Point Encryption Send-Key/Recv-Key. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute the password of Lupper with the password of Lupien because such a modification would have yielded the predictable result of mobile terminal authentication.

14. Claims 12, 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lupper, U.S. Publication No. 2003/0171112, in view of Chang, U.S. Patent No. 6,715,082, and further in view of Chan, U.S. Patent No. 7,197,765. Referring to claims 12, 13, Lupper does not disclose how the passwords are generated. Chan discloses generating passwords based on SHA hash information (abstract & Col. 3, line 17), which meets the limitation of calculating a hash value, SHA-1 hashing process. It would have been obvious to one of ordinary skill in the art at the time the invention was made to generate the passwords of Lupper using SHA-1 hash information in order to provide more secure passwords without requiring the user to memorize a large password as taught by Chan (Col. 1, lines 29-42).

15. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lupper, U.S. Publication No. 2003/0171112, in view of Chang, U.S. Patent No. 6,715,082, and in further view of Kalavade, U.S. Publication No. 2003/0051041. Referring to claim 17, Lupper discloses utilizing RADIUS and GPRS environments but does not disclose modifying RADIUS accounting data to generate GPRS accounting data. Kalavade discloses modifying RADIUS accounting data to generate GPRS accounting data ([0233]). It would have been obvious to one

of ordinary skill in the art at the time the invention was made to modify RADIUS accounting information in Lupper to generate GPRS accounting information in order to provide combined LAN/WAN based authentication on a single account and receive a single bill as taught by Kalavade ([0063]-[0066]).

16. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lupper, U.S. Publication No. 2003/0171112, in view of Chang, U.S. Patent No. 6,715,082, in view of Lupien, U.S. Patent No. 6,463,055, and further in view of Kalavade, U.S. Publication No. 2003/0051041. Referring to claim 19, Lupper discloses a generic WLAN architecture wherein a subscriber name and password are obtained from the subscriber and compared to locally available subscriber data records ([0078]), which meets the limitation of creating a password for a client, storing the password and identification information on a RADIUS server. The subscriber name and password are compared with the data records to determine whether the subscriber can use services in the local area network ([0080]). Authentication is performed by a RADIUS server ([0051]), which meets the limitation of utilizing the password and the identification information to authenticate the client on the RADIUS server. Lupper discloses that authentication includes utilizing a SIM card in communications with a server ([0092]), which meets the limitation of a smart card for a client. Lupper does not disclose that the passwords are one-time passwords. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use one-time entropy passwords in the WLAN of Lupper in order to reduce the security risks that are introduced from using fixed user information by using single use passwords that cannot be reused by an intruder as taught by Chang (Col. 2, lines 12-24). Chang does not disclose generating the one-time passwords using client identification information.

Lupien discloses a wireless network authentication system wherein a password is generated at a first station and compared with a password generated by a mobile terminal using the IMSI of the mobile terminal to authenticate the mobile terminal to access the network (Col. 10, line 56 – Col. 11, line 10), which meets the limitation of creating a password for a client based on identification information of the client. It would have been obvious to one of ordinary skill in the art at the time the invention was made to generate the one-time passwords suggested by Chang using the user identification information of Lupper because such a modification would have yielded the predictable result of mobile terminal authentication. Lupper discloses utilizing RADIUS and GPRS environments but does not disclose modifying RADIUS accounting data to generate GPRS accounting data. Kalavade discloses modifying RADIUS accounting data to generate GPRS accounting data ([0233]). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify RADIUS accounting information in Lupper to generate GPRS accounting information in order to provide combined LAN/WAN based authentication on a single account and receive a single bill as taught by Kalavade ([0063]-[0066]).

Conclusion

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN E. LANIER whose telephone number is (571)272-3805. The examiner can normally be reached on M-Th 6:00am-4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Benjamin E Lanier/
Primary Examiner, Art Unit 2132